United States Department of Agriculture

NRCS
Natural Resources Conservation Service
1201 NE Lloyd Blvd, Suite 900
Portland, Oregon 97232
Phone: 503 414 3200 Fax: 503 414 3103

July 16, 2007

Action Due: July 26, 2007

OREGON BULLETIN NO. OR-270-2007-1

SUBJECT: Information Resources Management

TO: NRCS Oregon Employees

Purpose: To transmit instruction on the treatment and handling of sensitive and private information.

Expiration Date: September 30, 2007

Background: Recently released National Bulletin 170-7-2 (should have been 270 – Information Resources Management) provided guidance on the handling and storage of private and sensitive information.

Examples of Private Data: Social Security number (SSN); tax ID; employee NFC ID; account numbers; and farm, tract, or common land unit (CLU) numbers.

Examples of Sensitive Data: name, address, or other geographic indicators; e-mail address; phone number; race; gender; ethnicity; disability; birth date.

Private and sensitive information must be requested and used only when the transaction cannot be completed without it; it must be entered for that one transaction only and not stored for any future use unless it is absolutely necessary. When private and sensitive information must be stored, it must be secured. If this information is on paper, it must be secured in a locked file cabinet or drawer where only authorized employees have access to it. If this information is in electronic form, the computer system, including laptops, tablets, and desktops; USB drives; external hard drives; and similar devices, whether they are encrypted or not, must be secured in a way that prevents the information from being lost or stolen. If the electronic files cannot be secured, the information must not be stored on that computer. The information may be best secured in an access-controlled, shared-drive folder on a physically secure server that is accessed over the network. Our intranet “Employees Only” site and the FTP server are not secured, so sensitive and private information must not be stored there.

Action: All employees will review files on their work station computers to assure that any file containing private and/or sensitive information is 1) necessary to retain, and 2) stored in a secure location from both electronic and physical theft. **Supervisors must report to Lesley Kelly, SAO by e-mail at lesley.kelly@or.usda.gov that their employees have removed or secured any sensitive and/or private data from their computers and that all paper copies of sensitive or private material is in locked storage so that the NRCS Oregon certification can be sent to National Headquarters by July 31, 2007.**

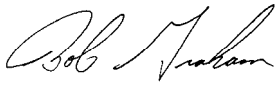
The following information will assist you with compliance to secure electronic files:

- The H:drive is a secure site
- The C: drive is only a secure site if documents are filed in the C:\Home directory or in the Documents and Settings folder, and these files have been encrypted.
- The S: drive is a secure site from outside users but any sensitive information should be protected by passwords for internal users.
- Thumb drives are only secure if encrypted.
- Do not save government information on home computers.

All employees will assure that "hard copy" files or documents containing private and/or sensitive are secured from access by non-authorized persons.

The following information will assist you with compliance to secure hard copy files:

- Do not leave files with private or sensitive information unsecured over night or when away from your workstation for an extended period.
- Private and or sensitive information needs to be shredded, not thrown in garbage cans or recycle barrels.



BOB GRAHAM
State Conservationist

cc:
Lesley Kelly, State Administrative Officer, NRCS Oregon, Portland, Oregon
Ardell Beier, USDA OCIO ITS Group Manager, Oregon/Idaho, Boise, Idaho